OIPE
SEP 14 2005
PATENT & TRADEMARK OFFICE
IAP87

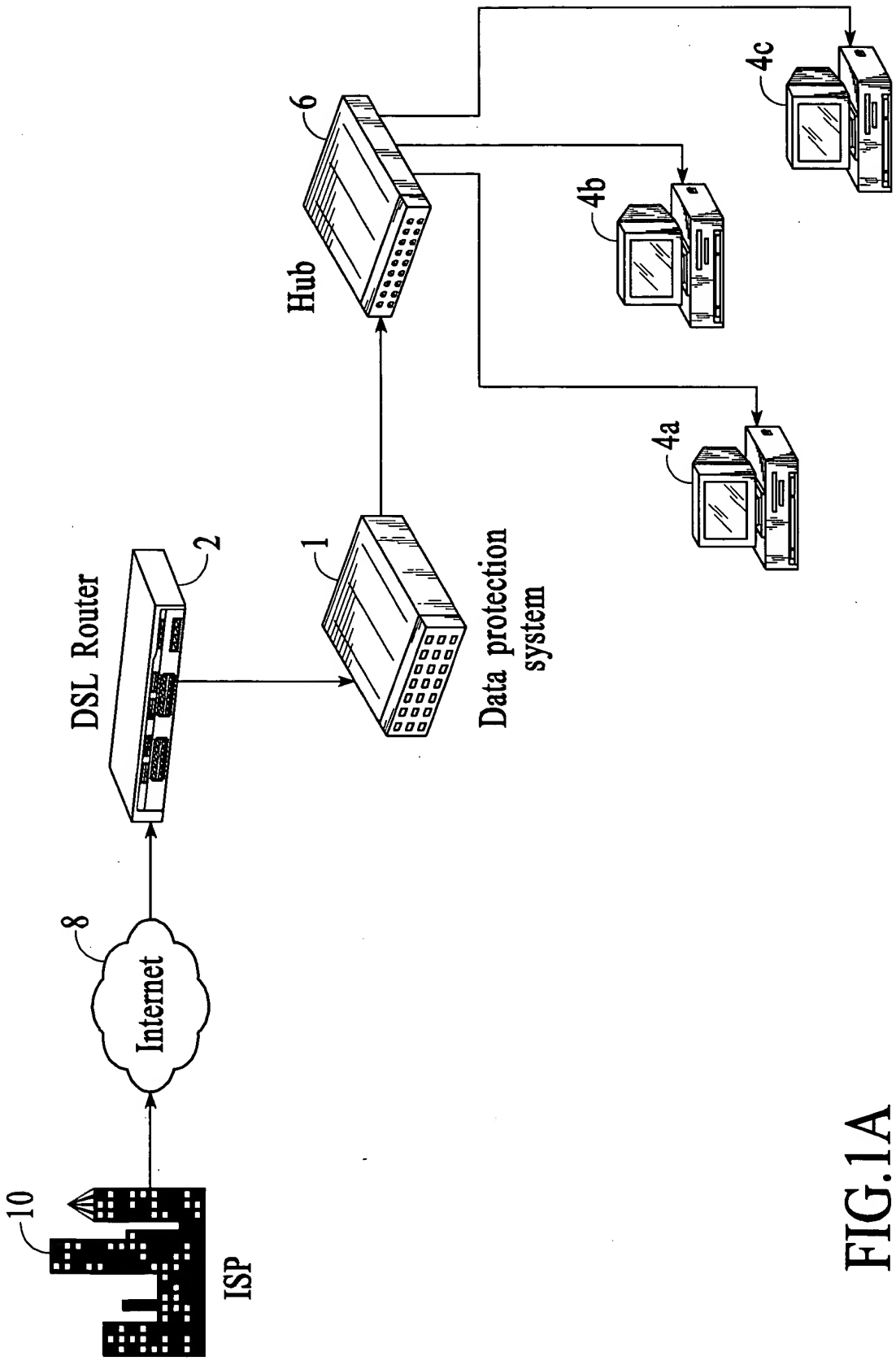


FIG.1A

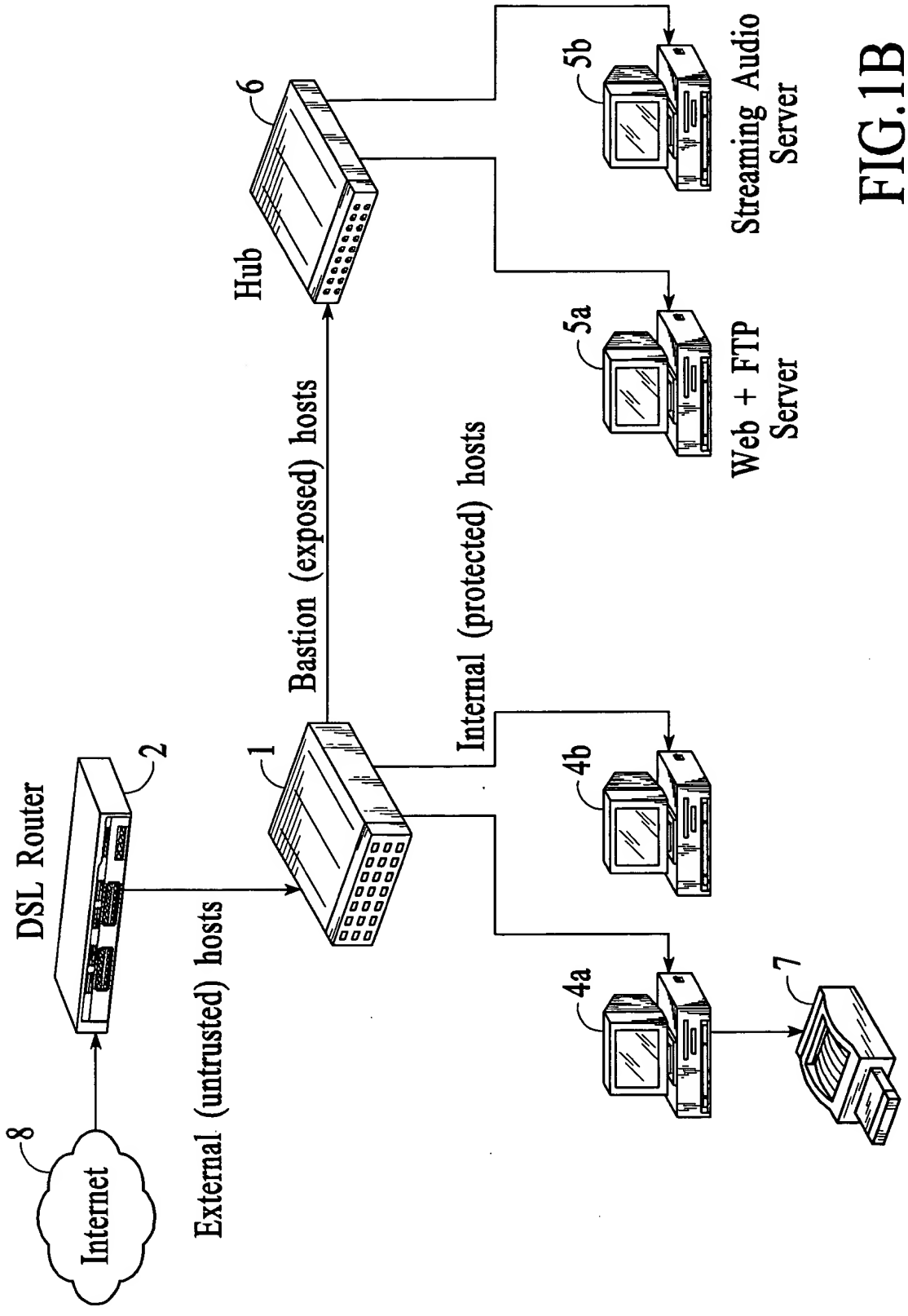

Internet
8
DSL Router
2
External (untrusted) hosts
1
Bastion (exposed) hosts
Internal (protected) hosts
Hub
6
4a
4b
5a
Web + FTP Server
5b
Streaming Audio Server
7

FIG.1B

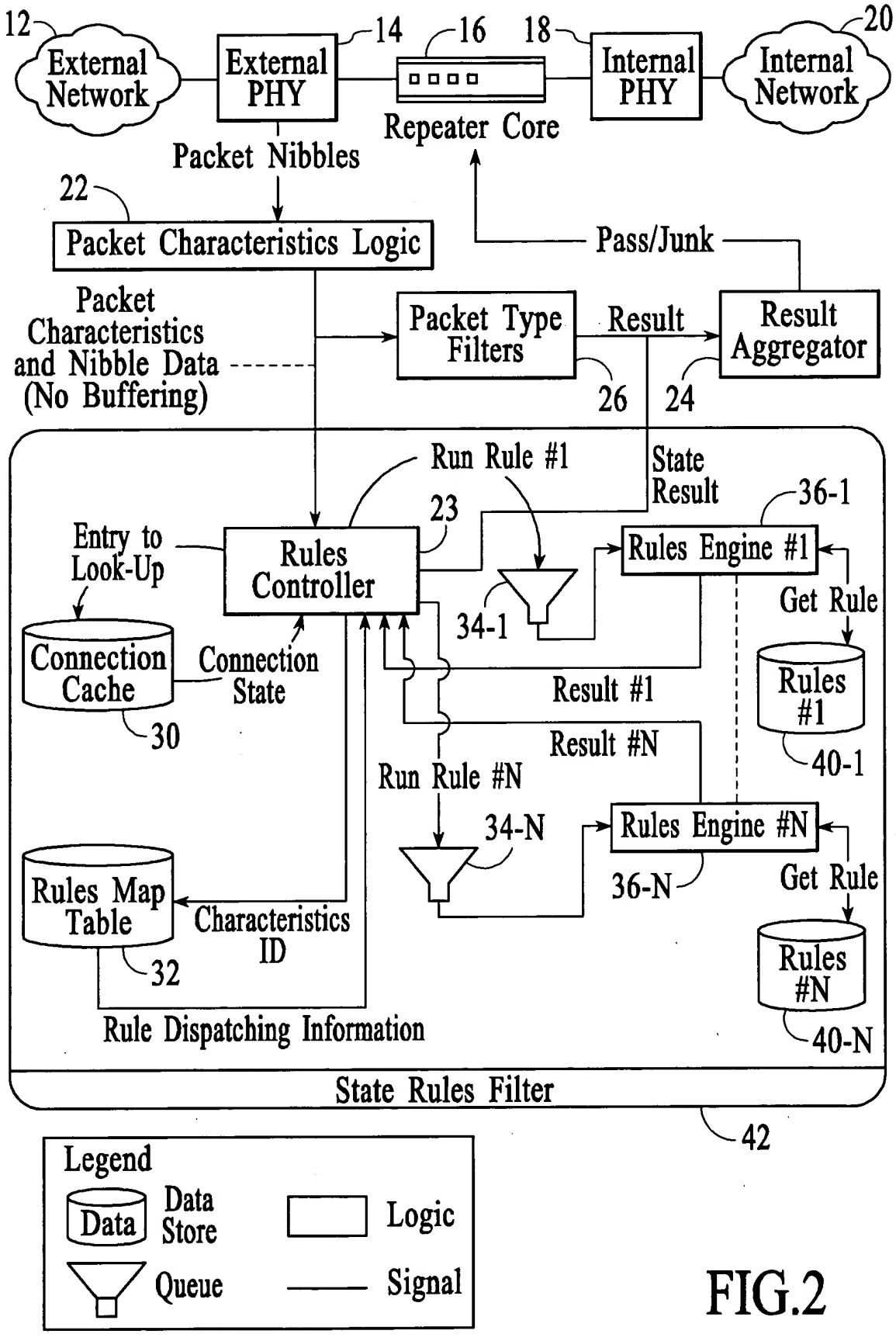

12
External Network
External PHY
14
16
18
Internal PHY
20
Internal Network
Repeater Core
Packet Nibbles
22
Packet Characteristics Logic
Pass/Junk
Packet Characteristics and Nibble Data (No Buffering)
Packet Type Filters
Result
Result Aggregator
26
24
Run Rule #1
State Result
23
36-1
Entry to Look-Up
Rules Controller
Rules Engine #1
Get Rule
34-1
Connection Cache
Connection State
Result #1
Rules #1
30
Result #N
40-1
Run Rule #N
34-N
Rules Engine #N
Rules Map Table
Characteristics ID
36-N
Get Rule
32
Rules #N
Rule Dispatching Information
40-N
State Rules Filter
42
Legend
Data
Data Store
Logic
Queue
Signal

FIG.2

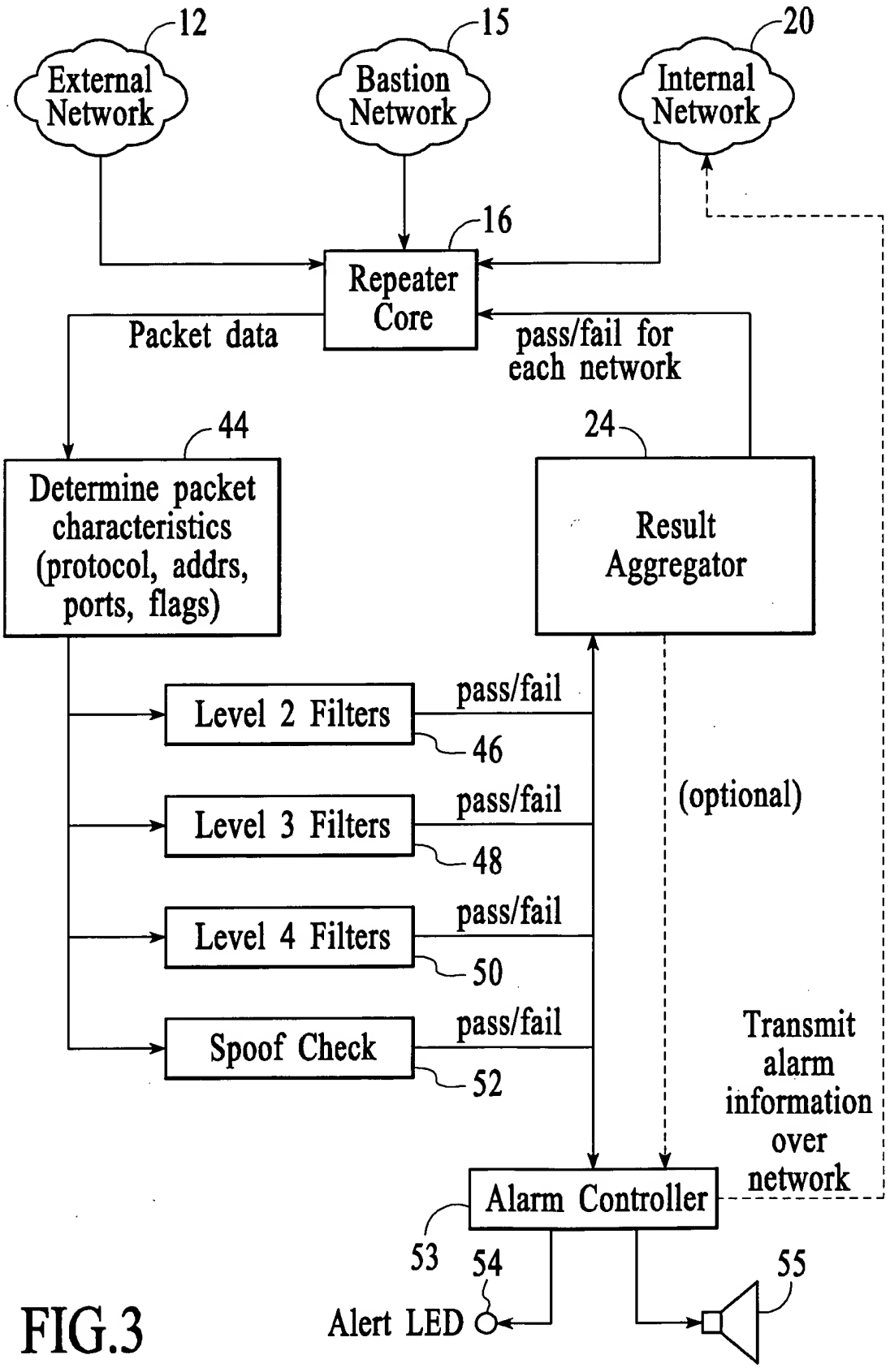
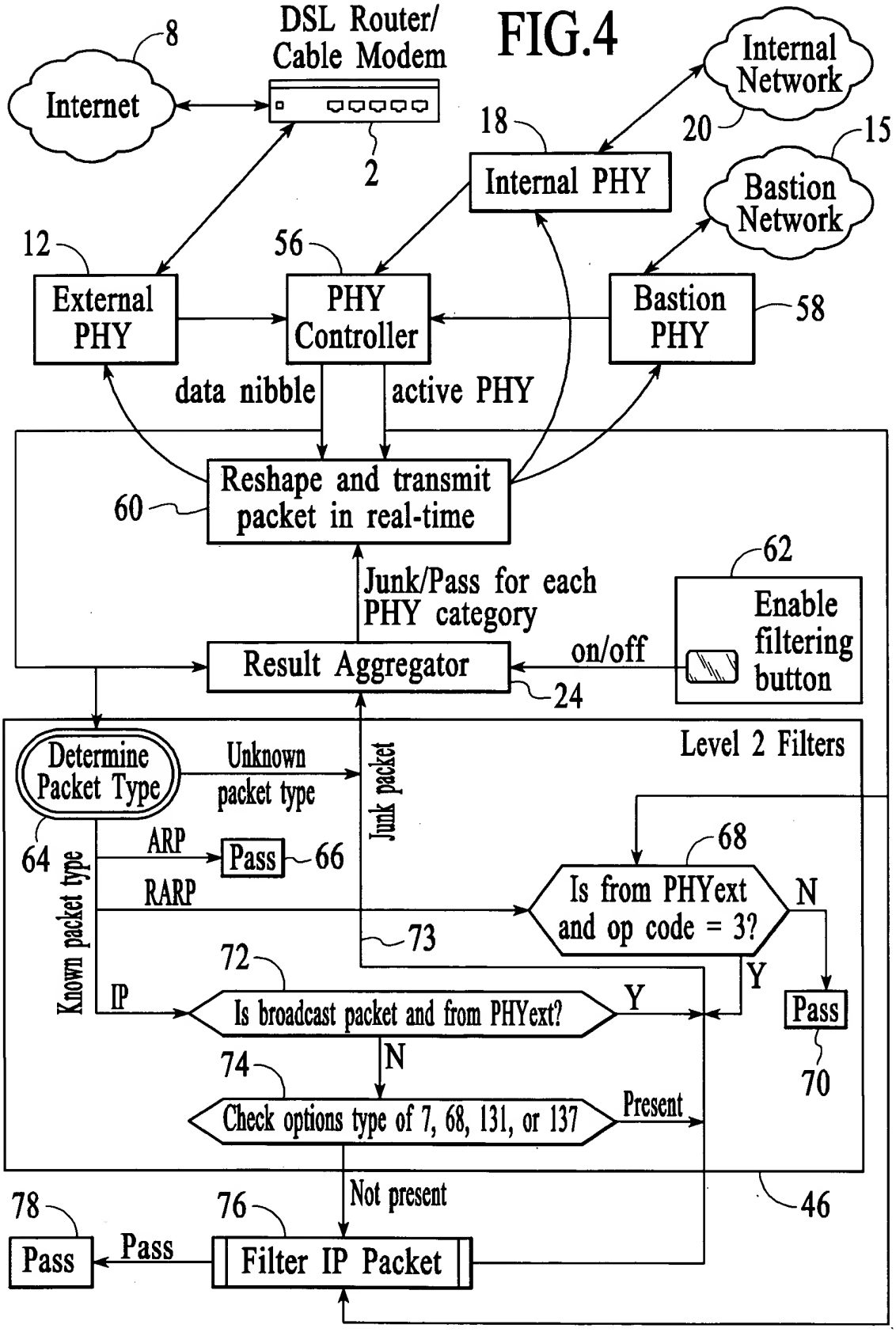

12
External Network
15
Bastion Network
20
Internal Network
16
Repeater Core
Packet data
pass/fail for each network
44
Determine packet characteristics (protocol, addrs, ports, flags)
24
Result Aggregator
Level 2 Filters
pass/fail
46
Level 3 Filters
pass/fail
48
Level 4 Filters
pass/fail
50
Spoof Check
pass/fail
52
(optional)
Transmit alarm information over network
Alarm Controller
53
54
Alert LED
55

FIG.3

FIG.4


DSL Router/
Cable Modem
8
Internet
2
Internal
Network
20
18
Internal PHY
15
Bastion
Network
12
External
PHY
56
PHY
Controller
Bastion
PHY
58
data nibble
active PHY
Reshape and transmit
packet in real-time
60
62
Junk/Pass for each
PHY category
Enable
filtering
button
on/off
Result Aggregator
24
Level 2 Filters
Determine
Packet Type
Unknown
packet type
Junk packet
64
ARP
Pass
66
RARP
Known packet type
68
Is from PHYext
and op code = 3?
N
Y
73
72
IP
Is broadcast packet and from PHYext?
Y
Pass
70
N
74
Check options type of 7, 68, 131, or 137
Present
Not present
46
78
76
Pass
Pass
Filter IP Packet

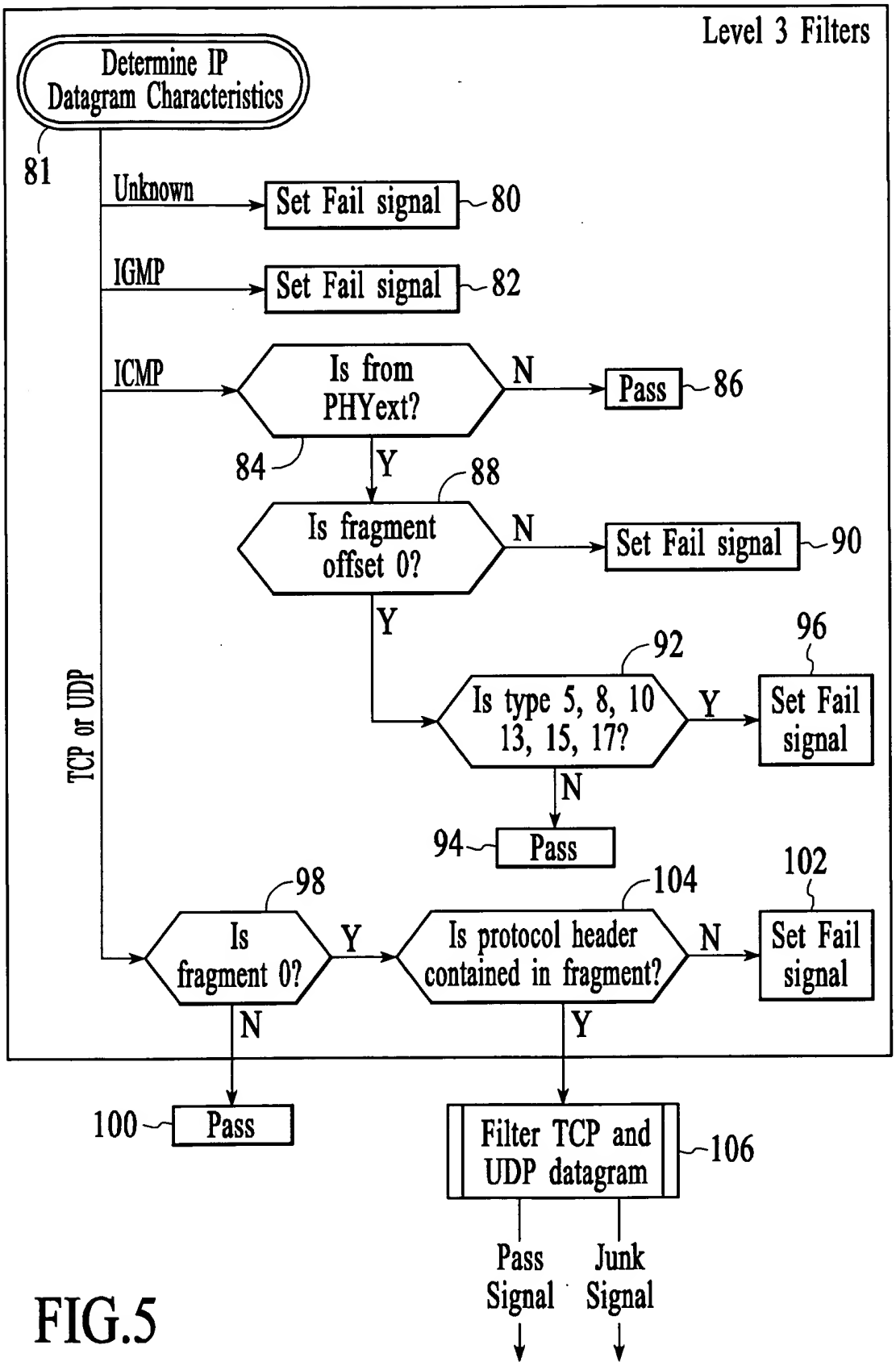

Level 3 Filters
Determine IP Datagram Characteristics
81
Unknown
Set Fail signal
80
IGMP
Set Fail signal
82
ICMP
Is from PHYext?
N
Pass
86
84
Y
88
Is fragment offset 0?
N
Set Fail signal
90
Y
92
96
Is type 5, 8, 10 13, 15, 17?
Y
Set Fail signal
N
94
Pass
TCP or UDP
98
104
102
Is fragment 0?
Y
Is protocol header contained in fragment?
N
Set Fail signal
N
Y
100
Pass
Filter TCP and UDP datagram
106
Pass Signal
Junk Signal

FIG.5

FIG.6

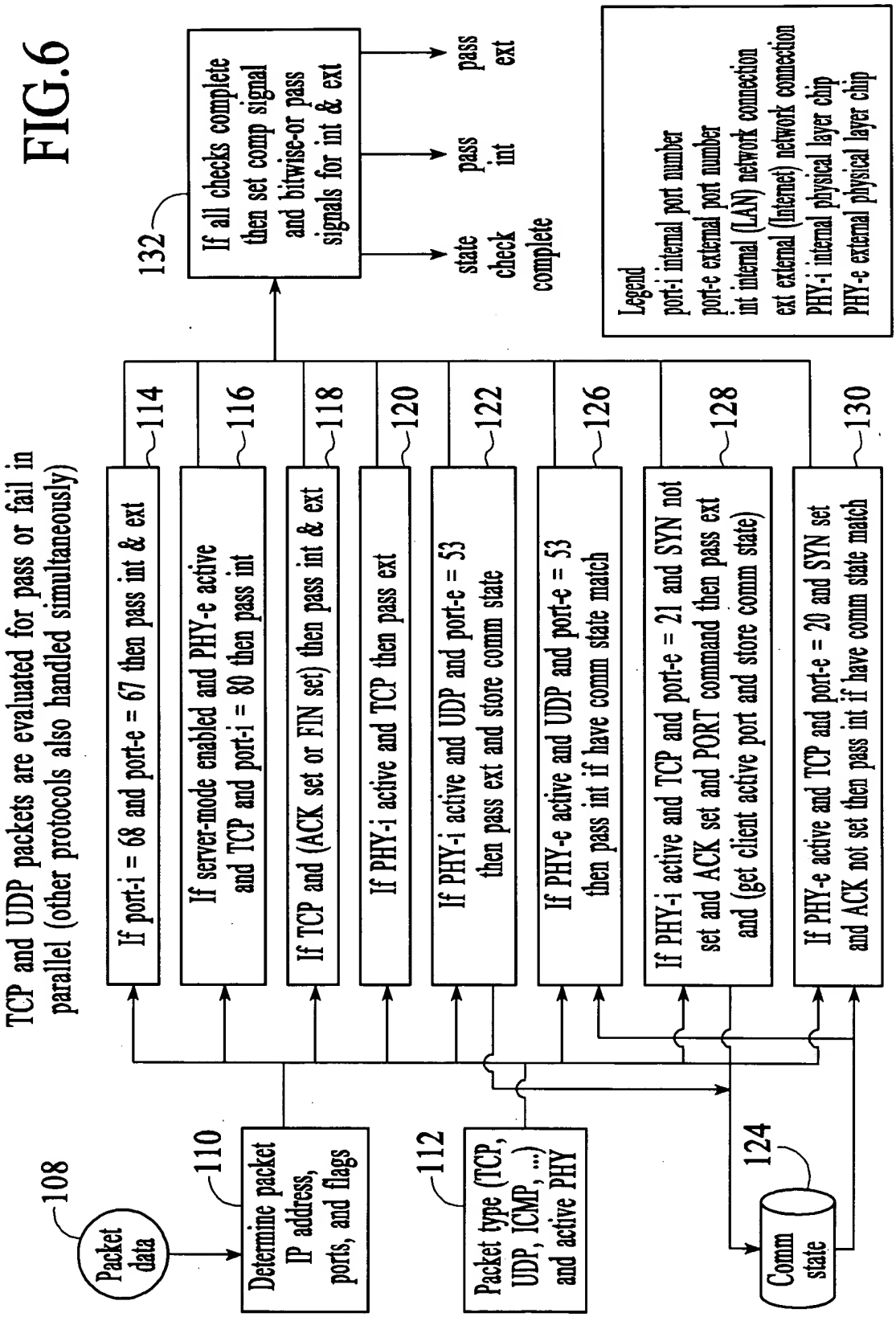
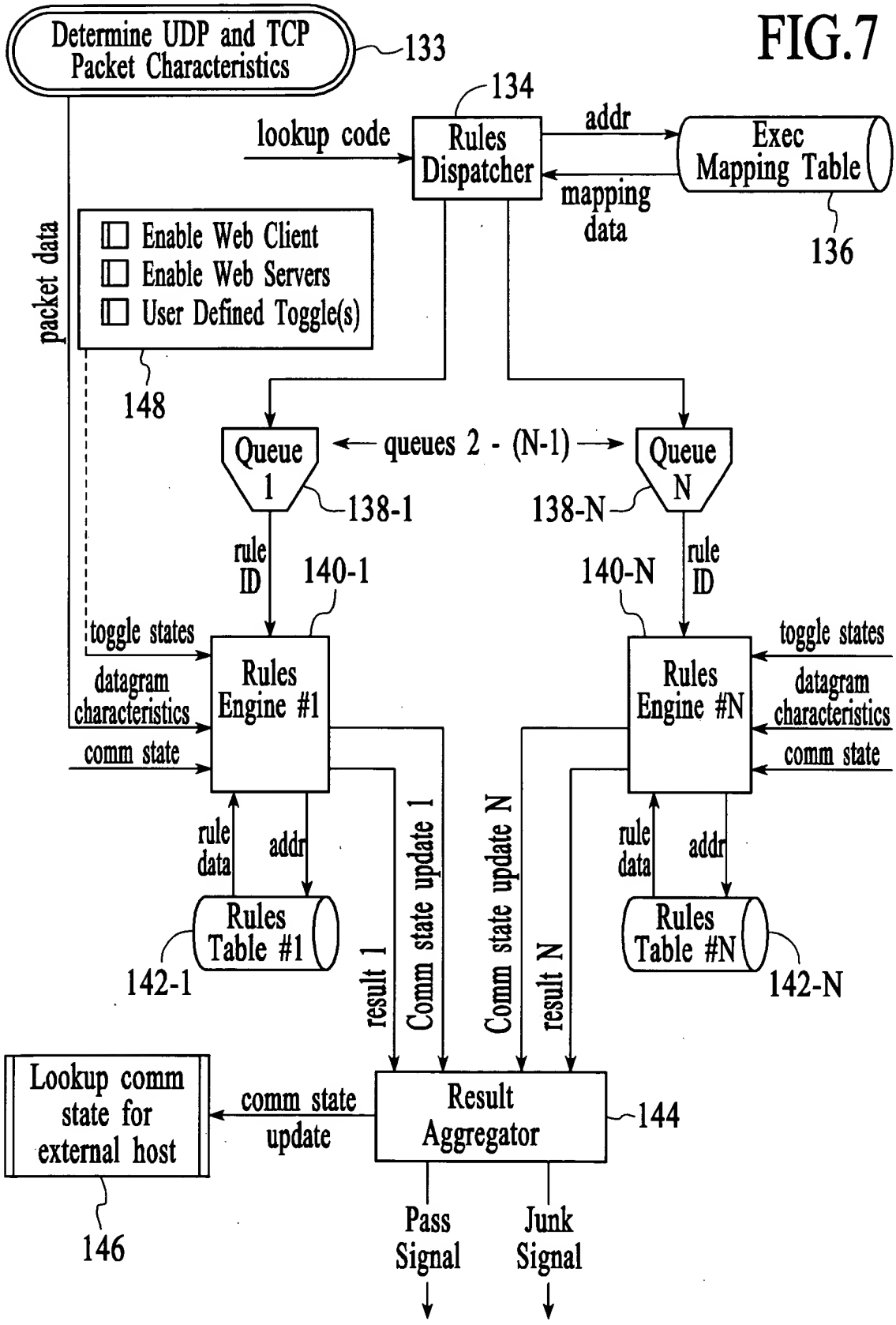

TCP and UDP packets are evaluated for pass or fail in parallel (other protocols also handled simultaneously)
108
Packet data
110
Determine packet IP address, ports, and flags
112
Packet type (TCP, UDP, ICMP, ...) and active PHY
124
Comm state
114
If port-i = 68 and port-e = 67 then pass int & ext
116
If server-mode enabled and PHY-e active and TCP and port-i = 80 then pass int
118
If TCP and (ACK set or FIN set) then pass int & ext
120
If PHY-i active and TCP then pass ext
122
If PHY-i active and UDP and port-e = 53 then pass ext and store comm state
126
If PHY-e active and UDP and port-e = 53 then pass int if have comm state match
128
If PHY-i active and TCP and port-e = 21 and SYN not set and ACK set and PORT command then pass ext and (get client active port and store comm state)
130
If PHY-e active and TCP and port-e = 20 and SYN set and ACK not set then pass int if have comm state match
132
If all checks complete then set comp signal and bitwise-or pass signals for int & ext
state check complete
pass int
pass ext
Legend
port-i internal port number
port-e external port number
int internal (LAN) network connection
ext external (Internet) network connection
PHY-i internal physical layer chip
PHY-e external physical layer chip

FIG.7


Determine UDP and TCP Packet Characteristics
133
134
lookup code
Rules Dispatcher
addr
mapping data
Exec Mapping Table
136
packet data
Enable Web Client
Enable Web Servers
User Defined Toggle(s)
148
Queue 1
queues 2 - (N-1)
Queue N
138-1
138-N
rule ID
140-1
140-N
rule ID
toggle states
datagram characteristics
comm state
Rules Engine #1
Rules Engine #N
toggle states
datagram characteristics
comm state
rule data
addr
rule data
addr
Rules Table #1
142-1
result 1
Comm state update 1
Comm state update N
result N
Rules Table #N
142-N
Lookup comm state for external host
comm state update
Result Aggregator
144
146
Pass Signal
Junk Signal

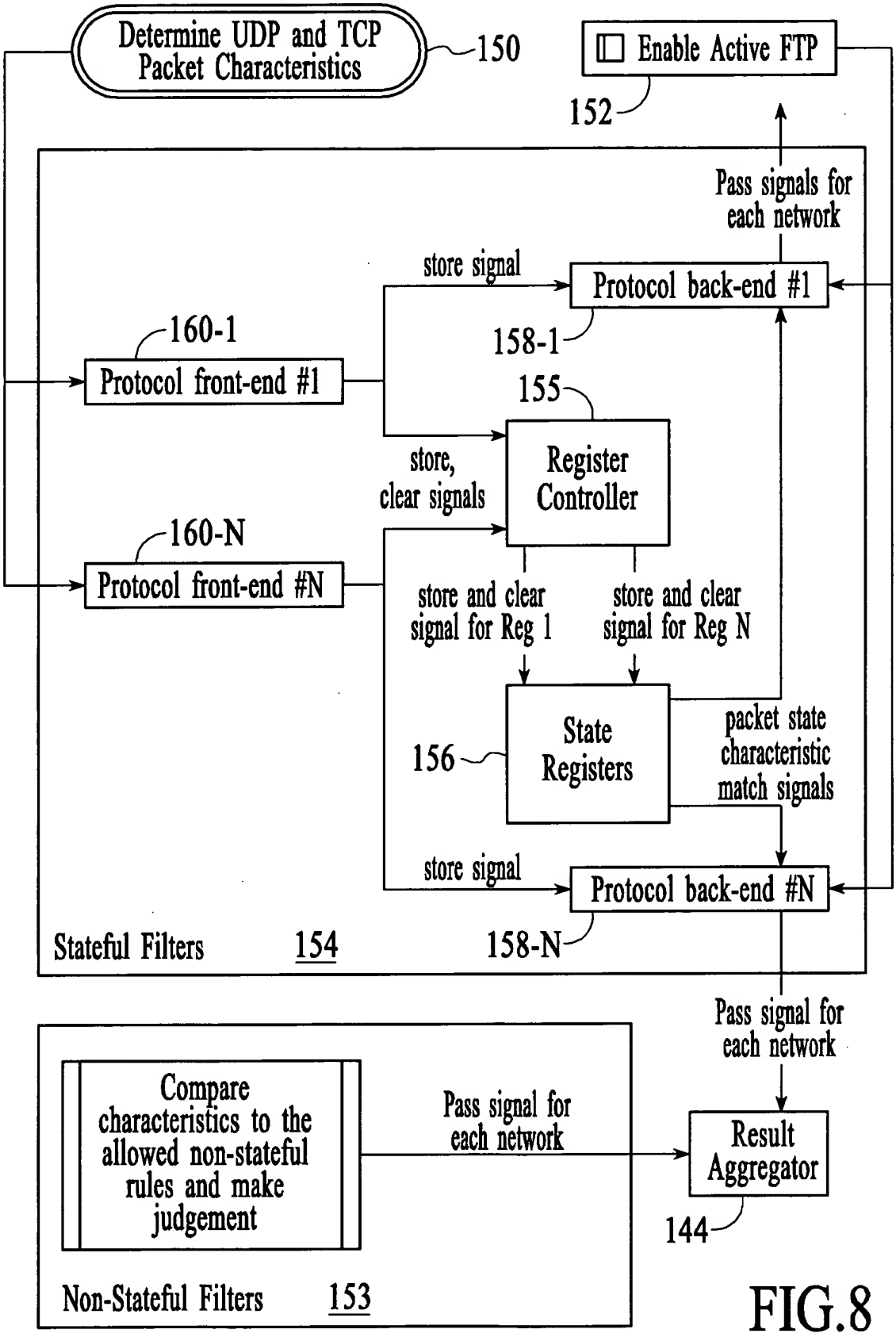

Determine UDP and TCP Packet Characteristics
150
Enable Active FTP
152
Pass signals for each network
store signal
Protocol back-end #1
158-1
160-1
Protocol front-end #1
155
Register Controller
store, clear signals
160-N
Protocol front-end #N
store and clear signal for Reg 1
store and clear signal for Reg N
State Registers
156
packet state characteristic match signals
store signal
Protocol back-end #N
158-N
Stateful Filters 154
Pass signal for each network
Compare characteristics to the allowed non-stateful rules and make judgement
Pass signal for each network
Result Aggregator
144
Non-Stateful Filters 153

FIG.8

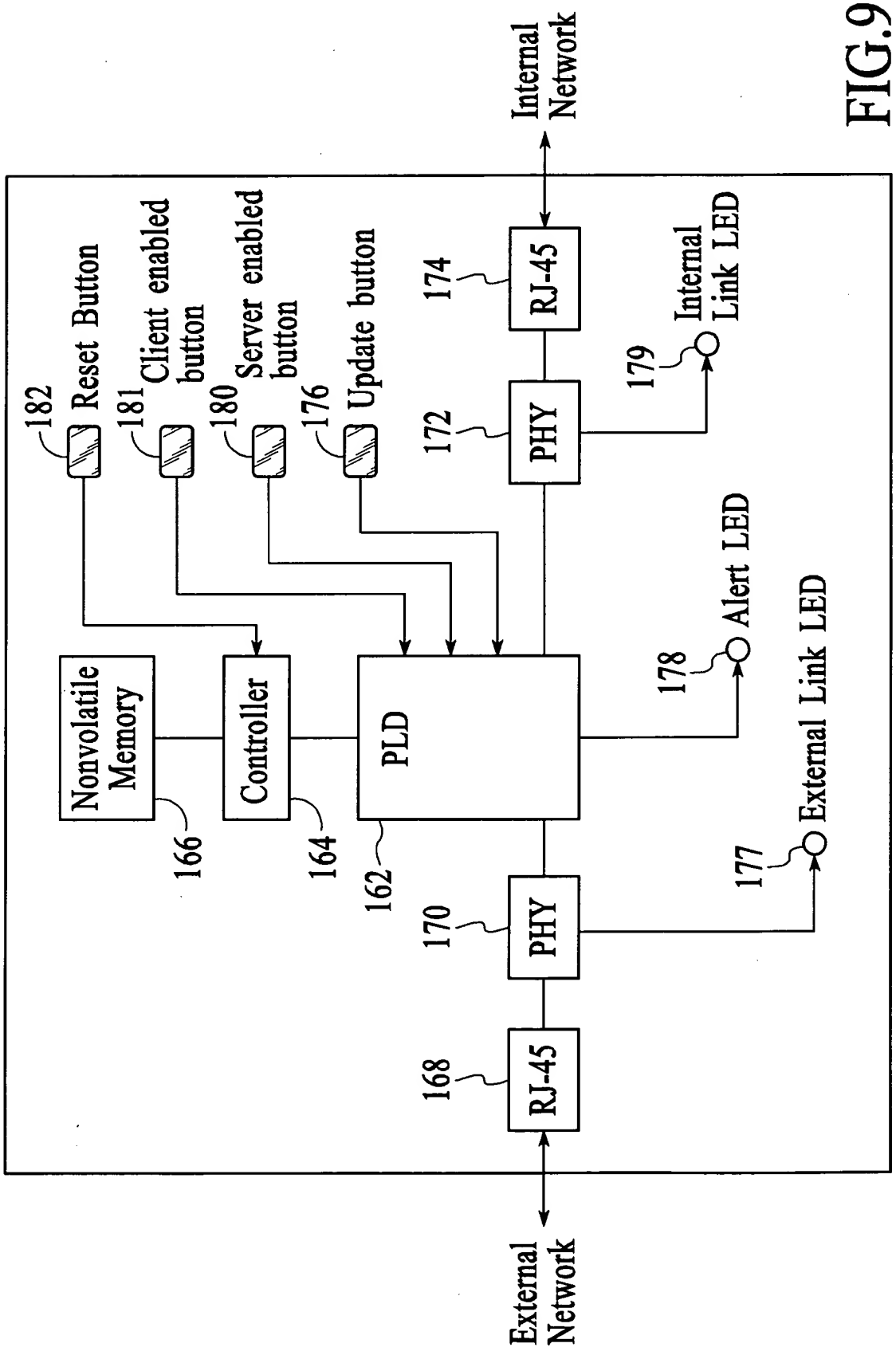

Internal Network
External Network
RJ-45
PHY
RJ-45
PHY
PLD
Controller
Nonvolatile Memory
Reset Button
Client enabled button
Server enabled button
Update button
Internal Link LED
Alert LED
External Link LED
174
172
170
168
162
164
166
182
181
180
176
179
178
177

FIG.9

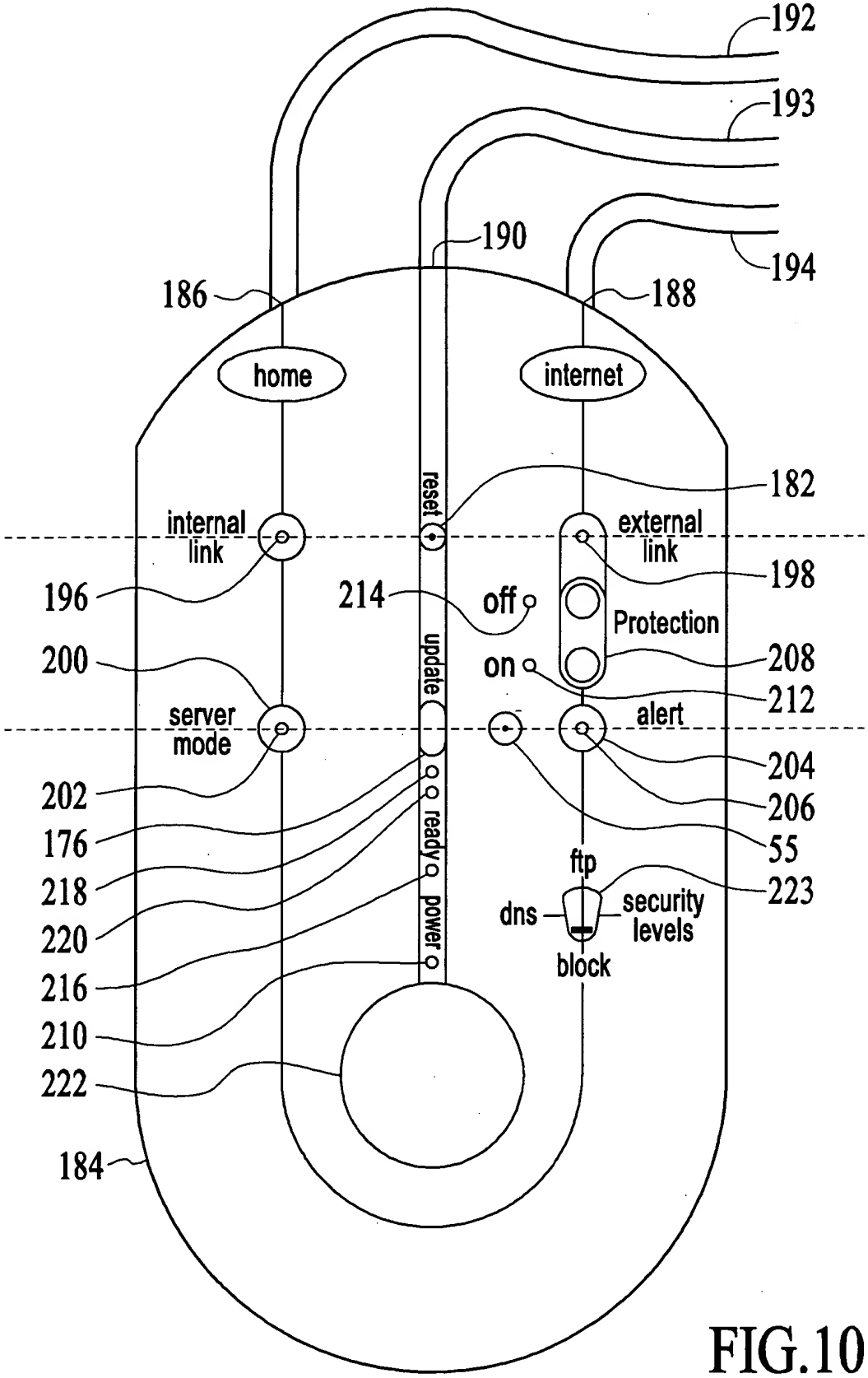

192
193
190
194
186
188
home
internet
182
reset
internal link
external link
198
196
214
off
Protection
200
update
on
208
212
server mode
alert
204
206
202
176
218
220
216
210
222
ready
power
55
ftp
223
dns
security levels
block
184

FIG.10

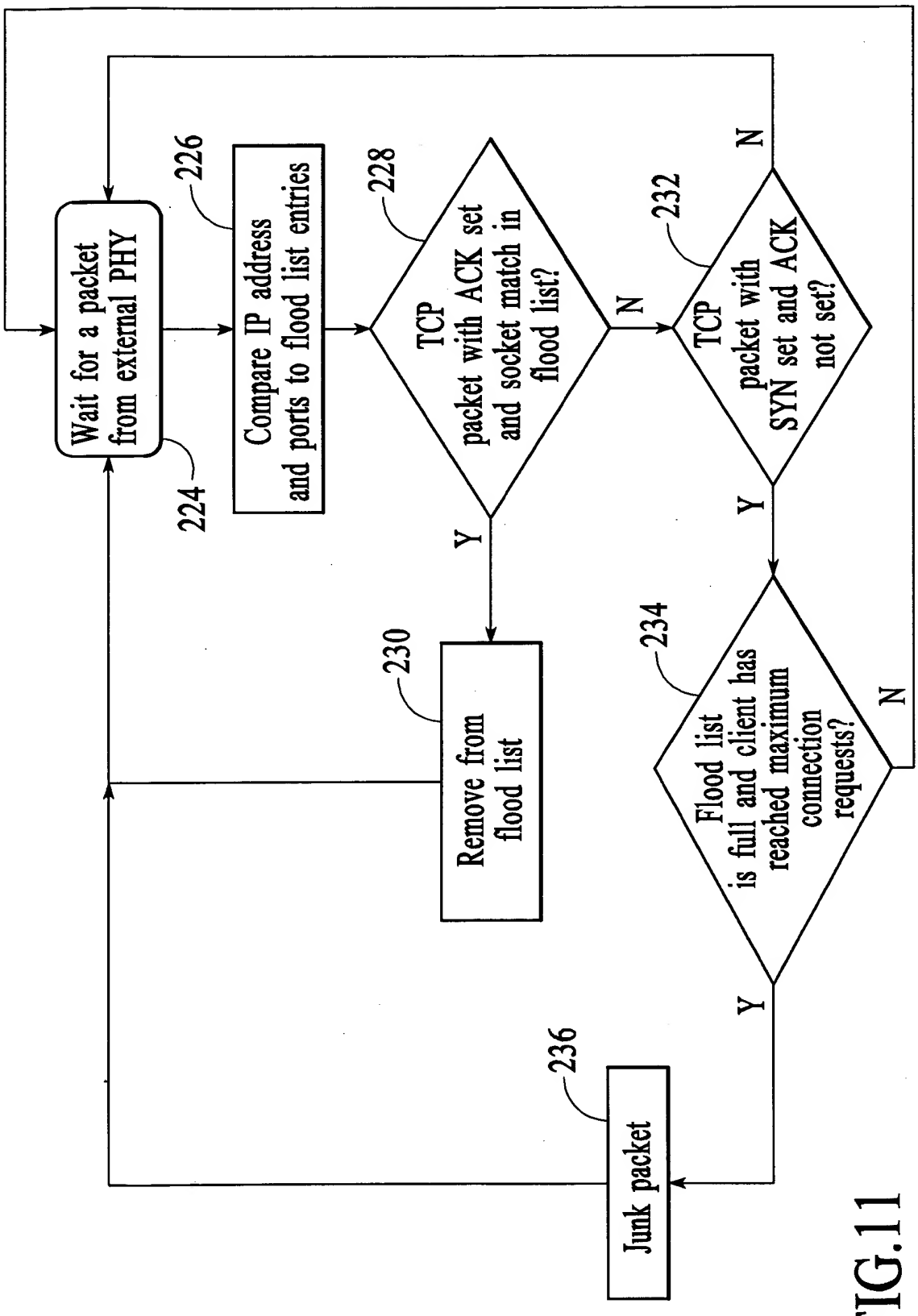

Wait for a packet from external PHY
224
Compare IP address and ports to flood list entries
226
TCP packet with ACK set and socket match in flood list?
228
Y
N
Remove from flood list
230
TCP packet with SYN set and ACK not set?
232
Y
N
Flood list is full and client has reached maximum connection requests?
234
Y
N
Junk packet
236

FIG.11

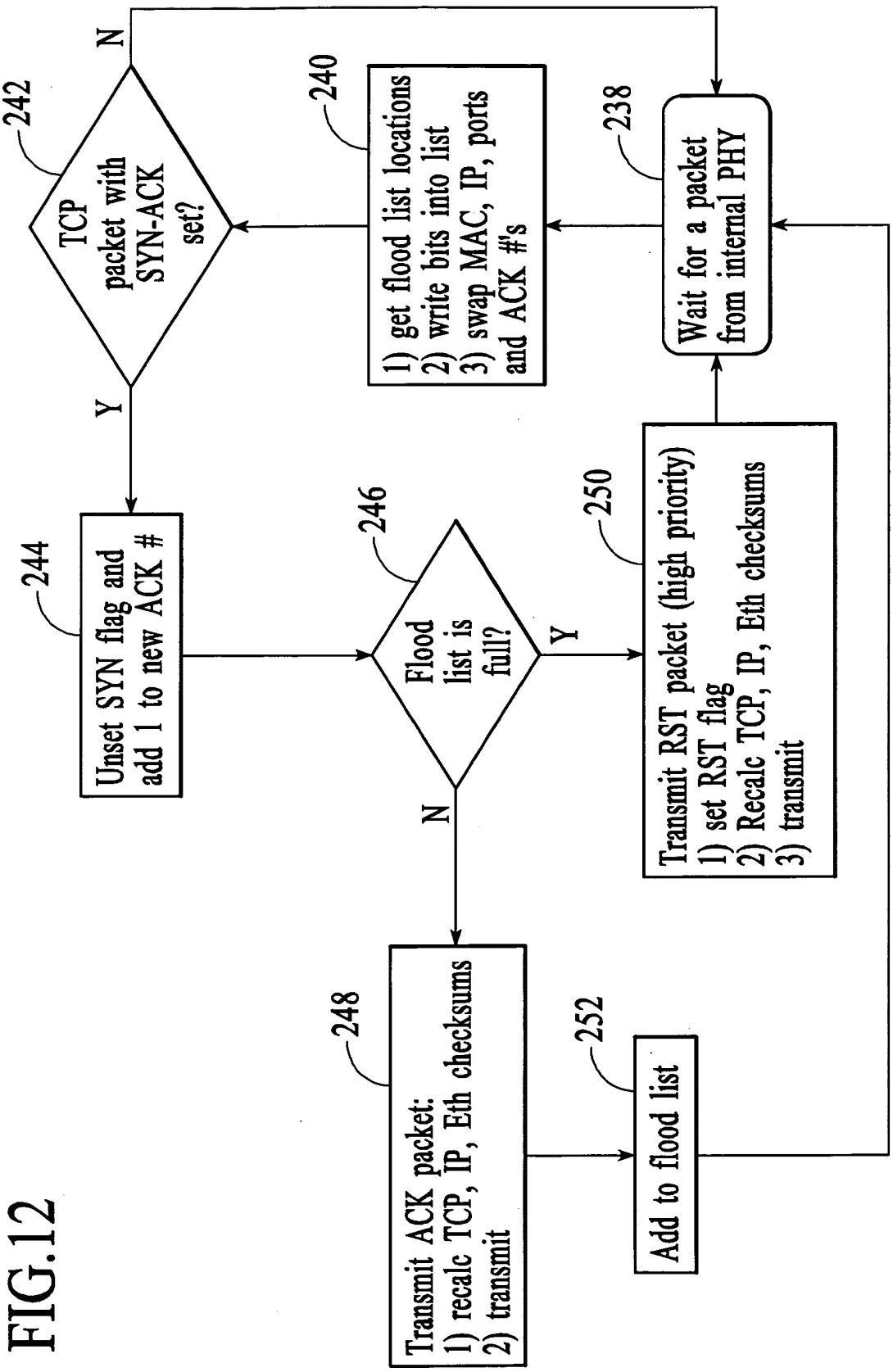

238
Wait for a packet from internal PHY
240
1) get flood list locations
2) write bits into list
3) swap MAC, IP, ports and ACK #'s
242
TCP packet with SYN-ACK set?
N
Y
244
Unset SYN flag and add 1 to new ACK #
246
Flood list is full?
Y
N
250
Transmit RST packet (high priority)
1) set RST flag
2) Recalc TCP, IP, Eth checksums
3) transmit
248
Transmit ACK packet:
1) recalc TCP, IP, Eth checksums
2) transmit
252
Add to flood list

FIG.12

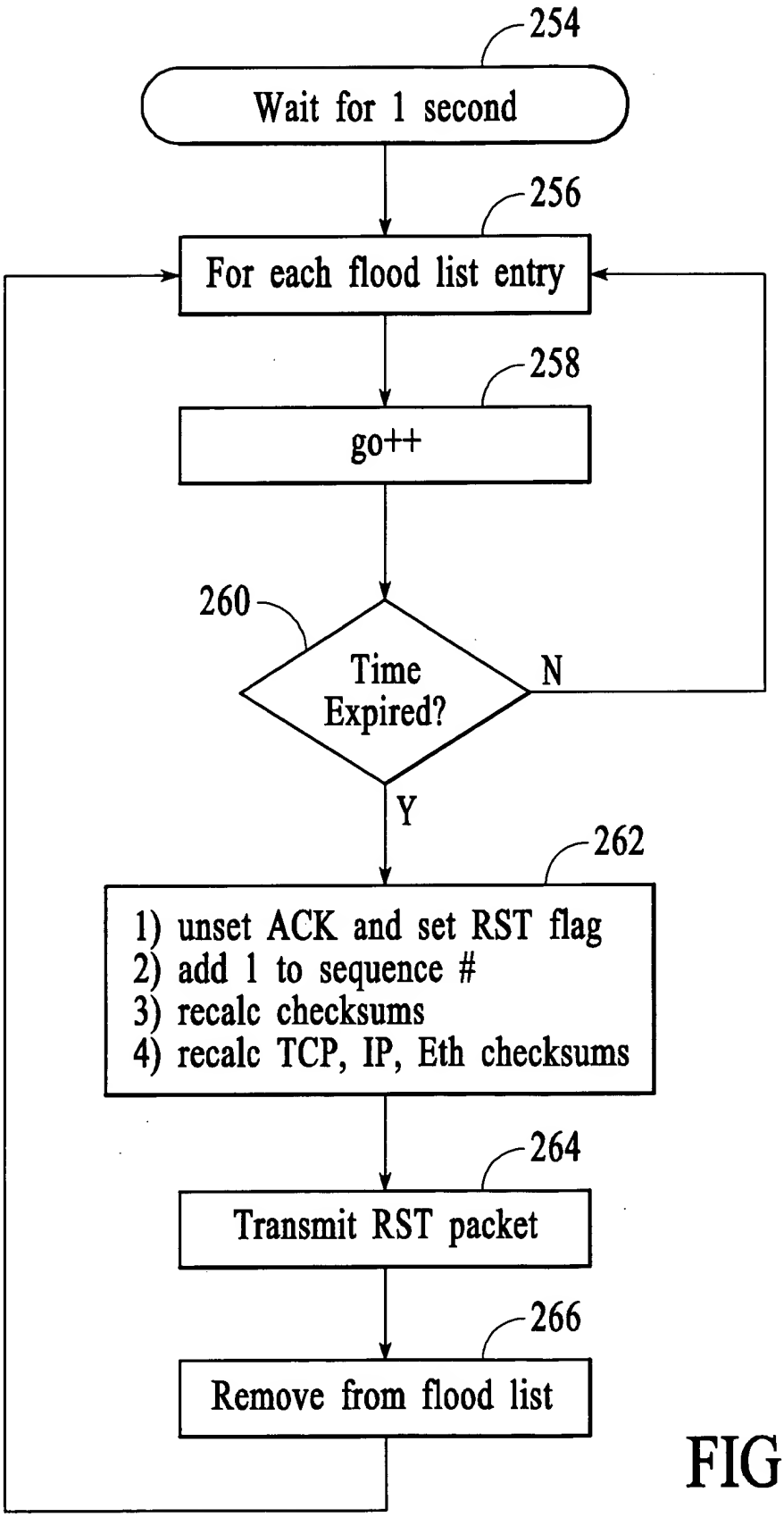

254
Wait for 1 second
256
For each flood list entry
258
go++
260
Time Expired?
N
Y
262
1) unset ACK and set RST flag
2) add 1 to sequence #
3) recalc checksums
4) recalc TCP, IP, Eth checksums
264
Transmit RST packet
266
Remove from flood list

FIG.13

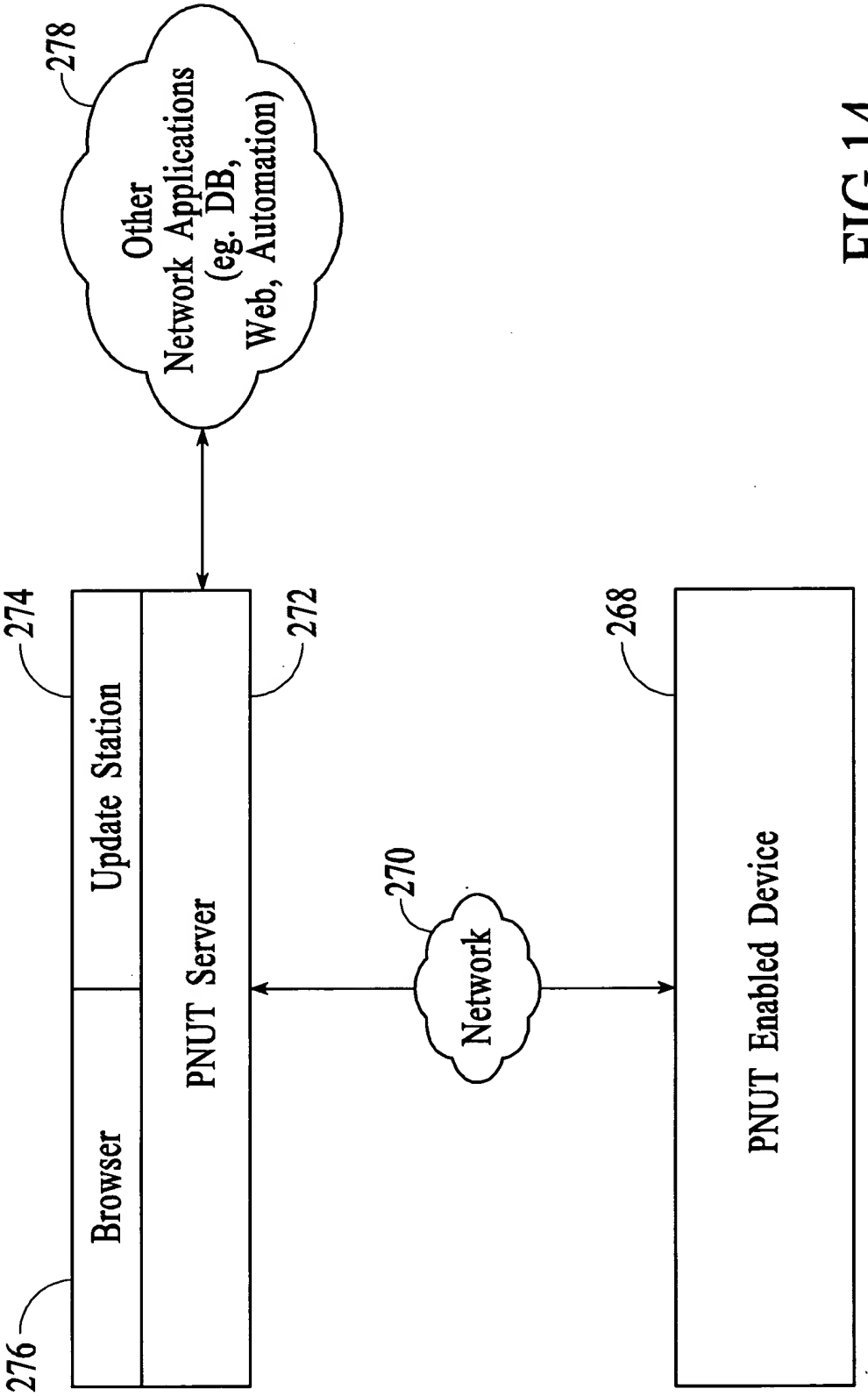

278
Other
Network Applications
(eg. DB,
Web, Automation)
274
Update Station
272
PNUT Server
270
Network
268
PNUT Enabled Device
Browser
276

FIG.14

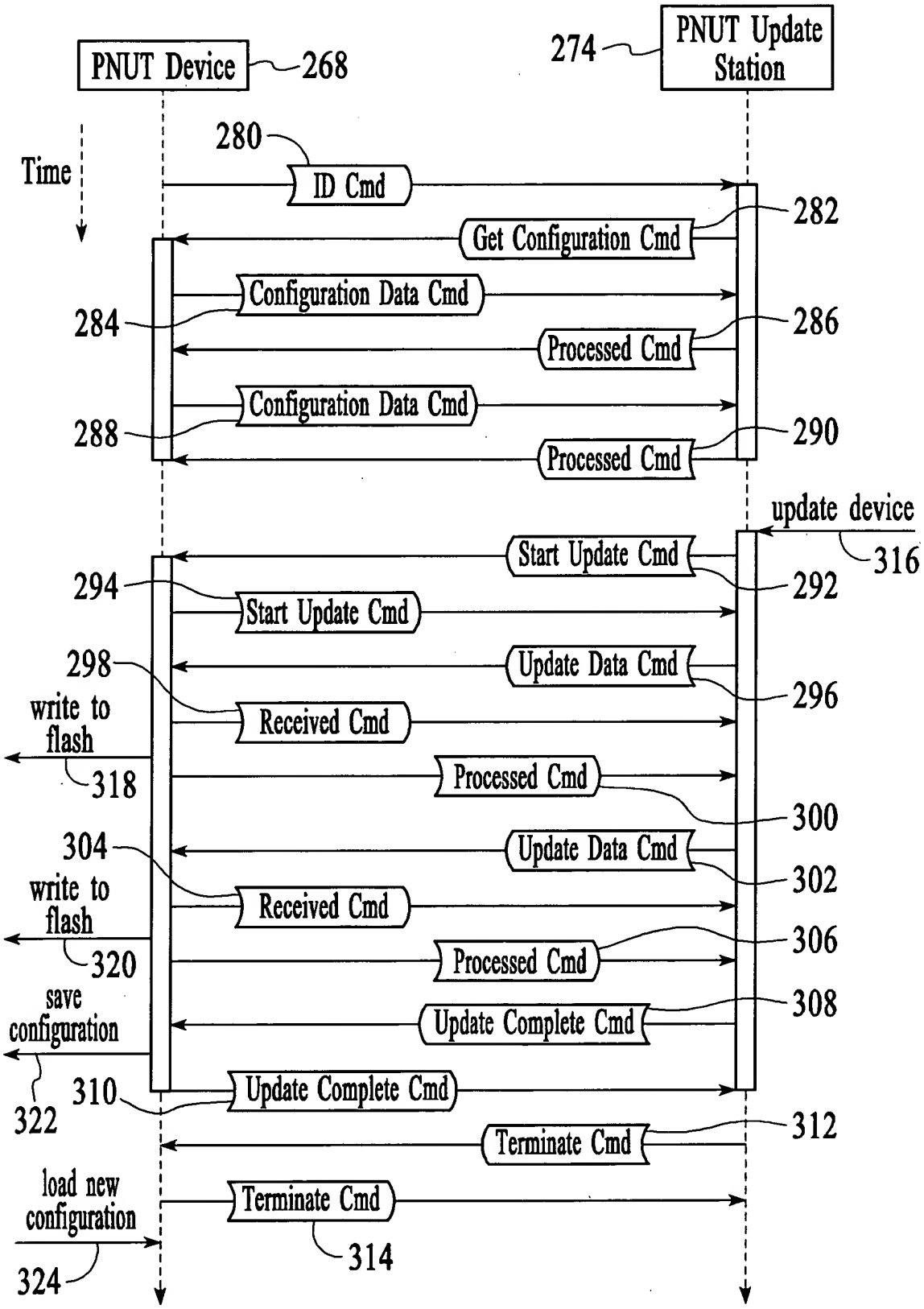

PNUT Device
268
274
PNUT Update Station
Time
280
ID Cmd
Get Configuration Cmd
282
Configuration Data Cmd
284
Processed Cmd
286
Configuration Data Cmd
288
Processed Cmd
290
update device
316
Start Update Cmd
292
294
Start Update Cmd
Update Data Cmd
298
296
write to flash
Received Cmd
318
Processed Cmd
300
Update Data Cmd
304
302
write to flash
Received Cmd
320
Processed Cmd
306
save configuration
Update Complete Cmd
308
322
310
Update Complete Cmd
Terminate Cmd
312
load new configuration
Terminate Cmd
314
324

FIG.15

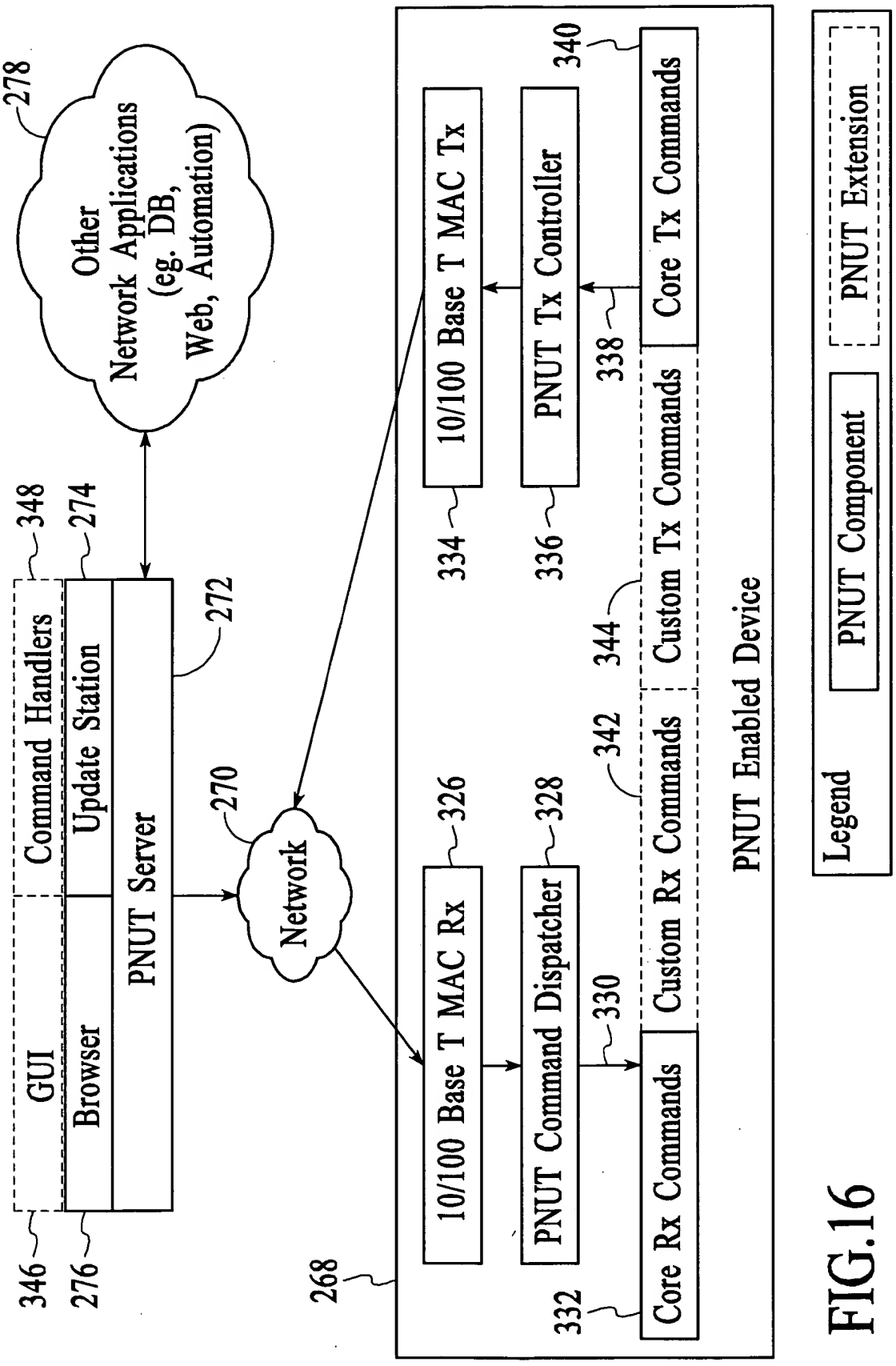
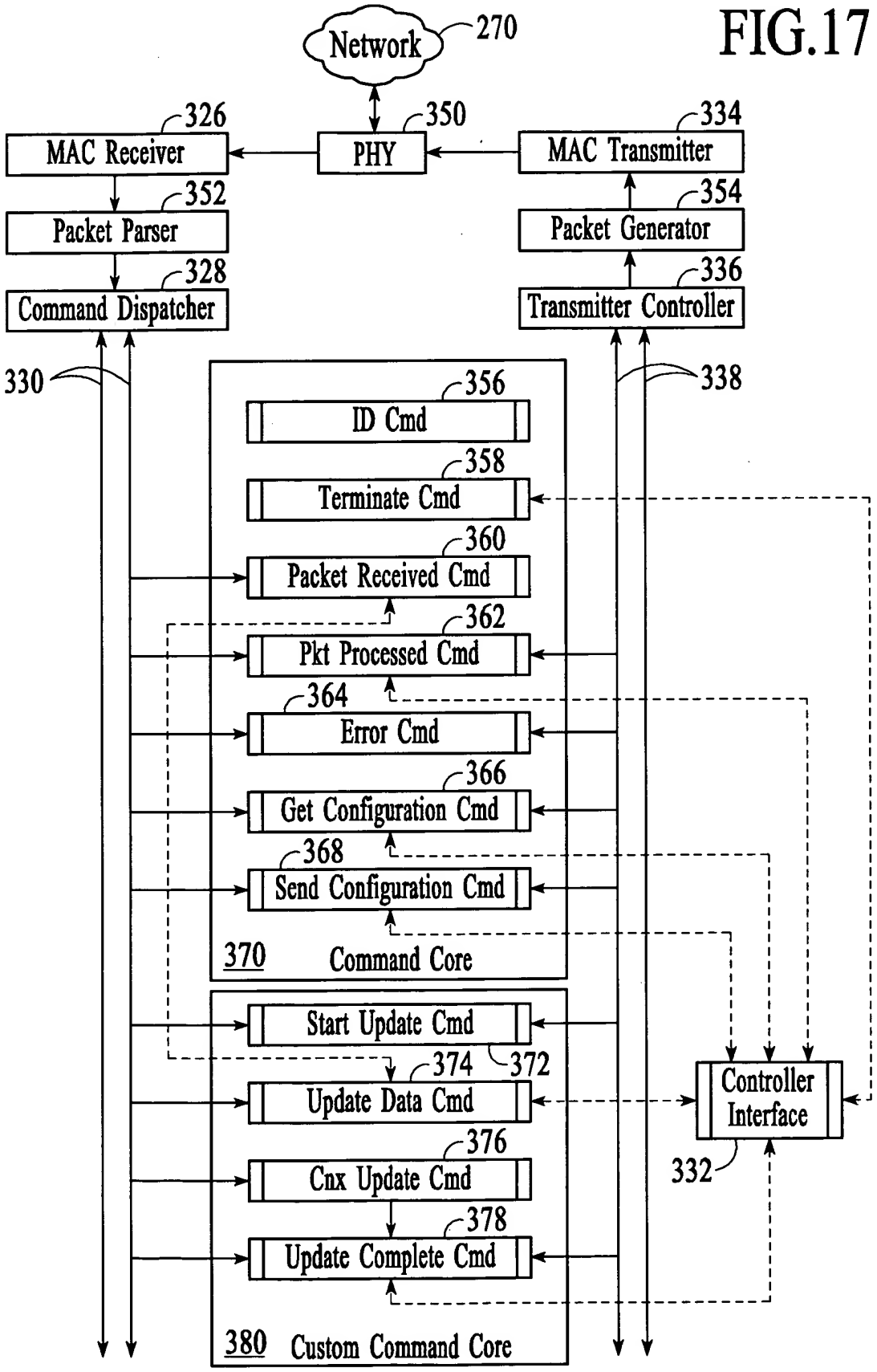

278
Other
Network Applications
(eg. DB,
Web, Automation)
348
274
Command Handlers
Update Station
Browser
PNUT Server
272
346
276
270
Network
268
10/100 Base T MAC Rx
326
PNUT Command Dispatcher
328
330
Core Rx Commands
Custom Rx Commands
342
332
10/100 Base T MAC Tx
334
PNUT Tx Controller
336
Core Tx Commands
Custom Tx Commands
340
338
344
PNUT Enabled Device
Legend
PNUT Component
PNUT Extension

FIG.16

FIG.17


Network
270
326
MAC Receiver
350
PHY
334
MAC Transmitter
352
Packet Parser
354
Packet Generator
328
Command Dispatcher
336
Transmitter Controller
330
338
356
ID Cmd
358
Terminate Cmd
360
Packet Received Cmd
362
Pkt Processed Cmd
364
Error Cmd
366
Get Configuration Cmd
368
Send Configuration Cmd
370
Command Core
Start Update Cmd
372
374
Update Data Cmd
376
Cnx Update Cmd
378
Update Complete Cmd
380
Custom Command Core
Controller Interface
332

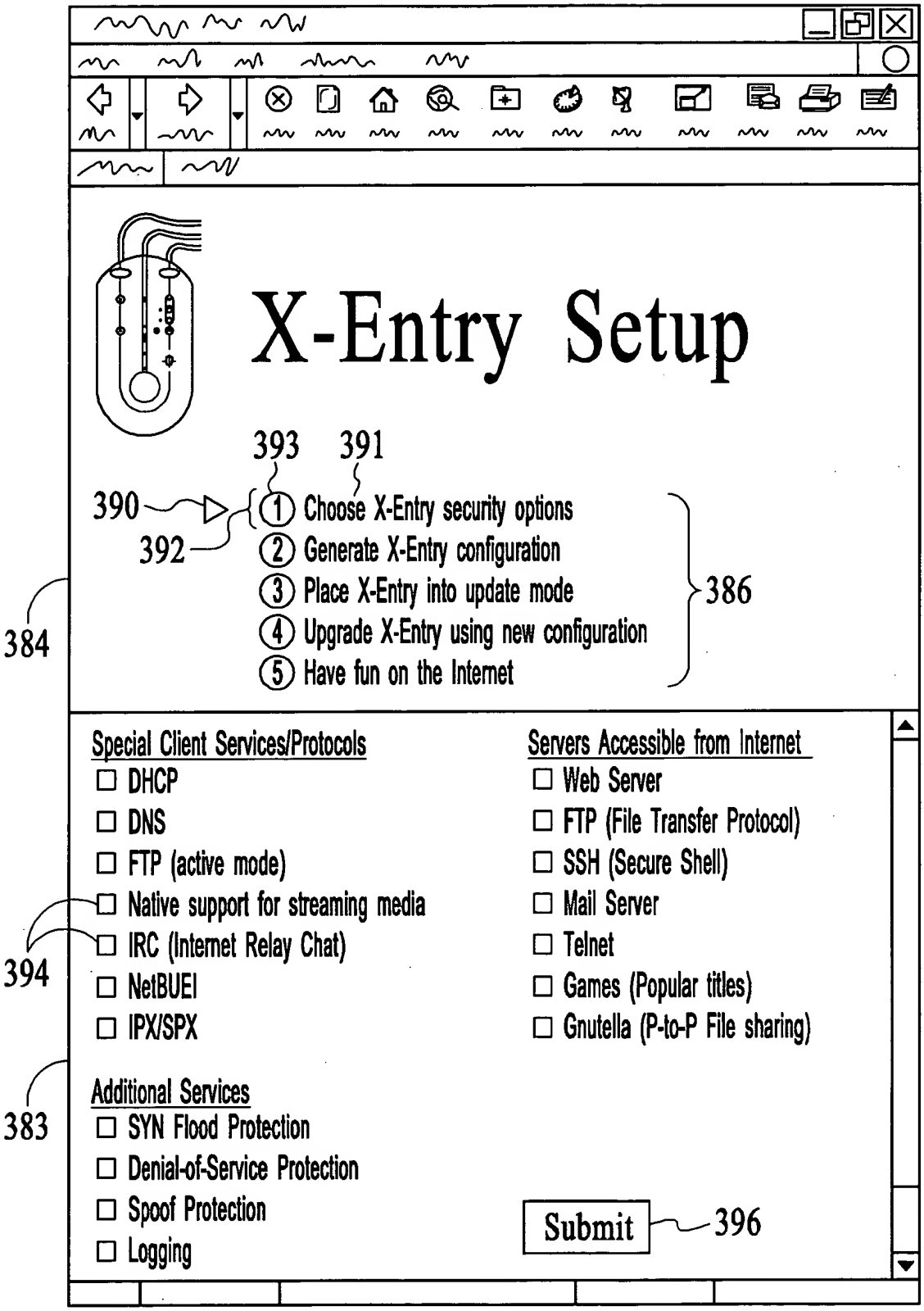

X-Entry Setup
393
391
390
392
1 Choose X-Entry security options
2 Generate X-Entry configuration
3 Place X-Entry into update mode
4 Upgrade X-Entry using new configuration
5 Have fun on the Internet
386
384
Special Client Services/Protocols
DHCP
DNS
FTP (active mode)
Native support for streaming media
IRC (Internet Relay Chat)
NetBUEI
IPX/SPX
394
Servers Accessible from Internet
Web Server
FTP (File Transfer Protocol)
SSH (Secure Shell)
Mail Server
Telnet
Games (Popular titles)
Gnutella (P-to-P File sharing)
Additional Services
383
SYN Flood Protection
Denial-of-Service Protection
Spoof Protection
Logging
Submit
396

FIG.18

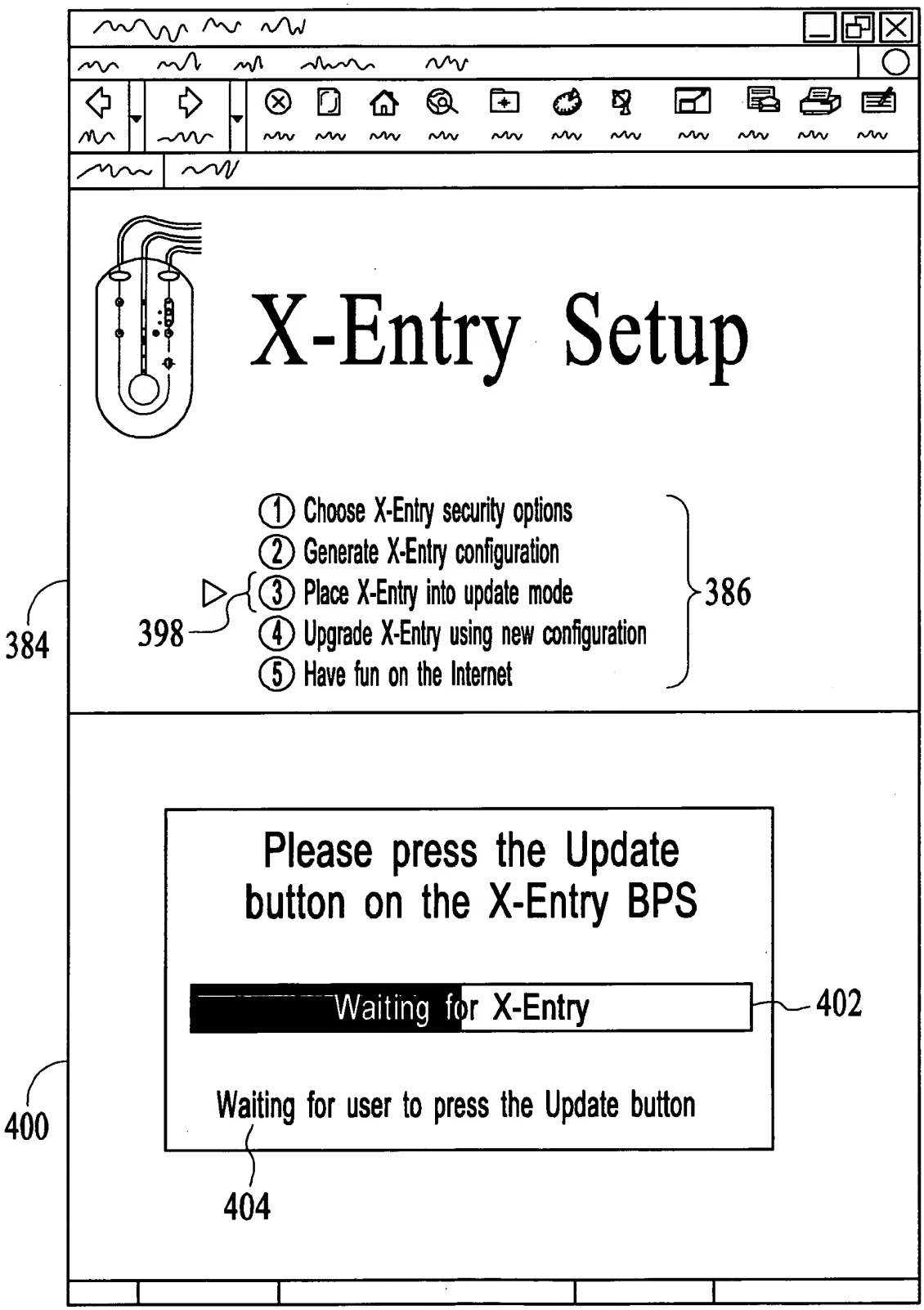

X-Entry Setup
1 Choose X-Entry security options
2 Generate X-Entry configuration
3 Place X-Entry into update mode
4 Upgrade X-Entry using new configuration
5 Have fun on the Internet
384
398
386
Please press the Update button on the X-Entry BPS
Waiting for X-Entry
402
400
Waiting for user to press the Update button
404

FIG.19

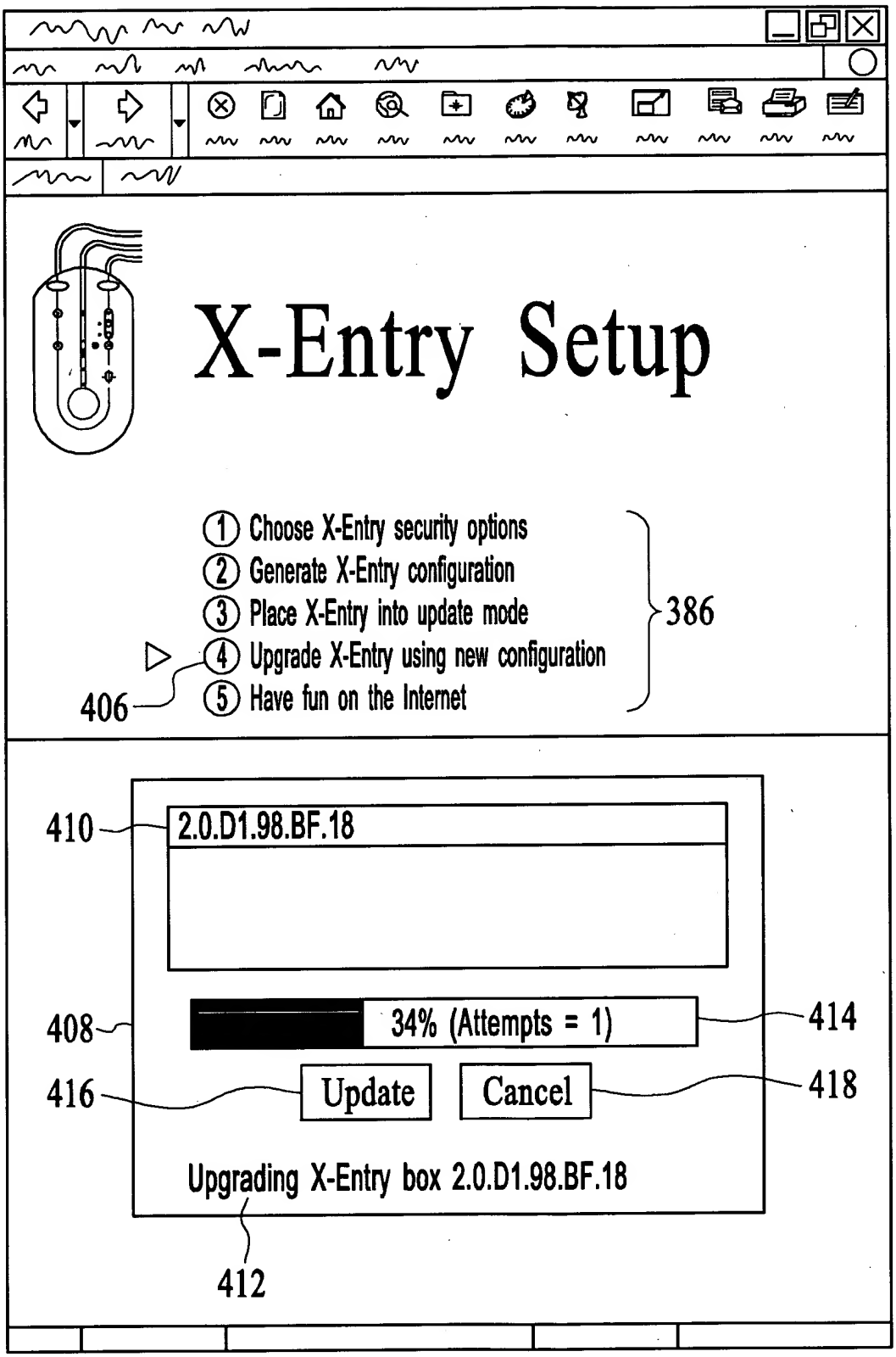

X-Entry Setup
1 Choose X-Entry security options
2 Generate X-Entry configuration
3 Place X-Entry into update mode
4 Upgrade X-Entry using new configuration
5 Have fun on the Internet
386
406
410
2.0.D1.98.BF.18
408
34% (Attempts = 1)
414
416
Update
Cancel
418
Upgrading X-Entry box 2.0.D1.98.BF.18
412

FIG.20

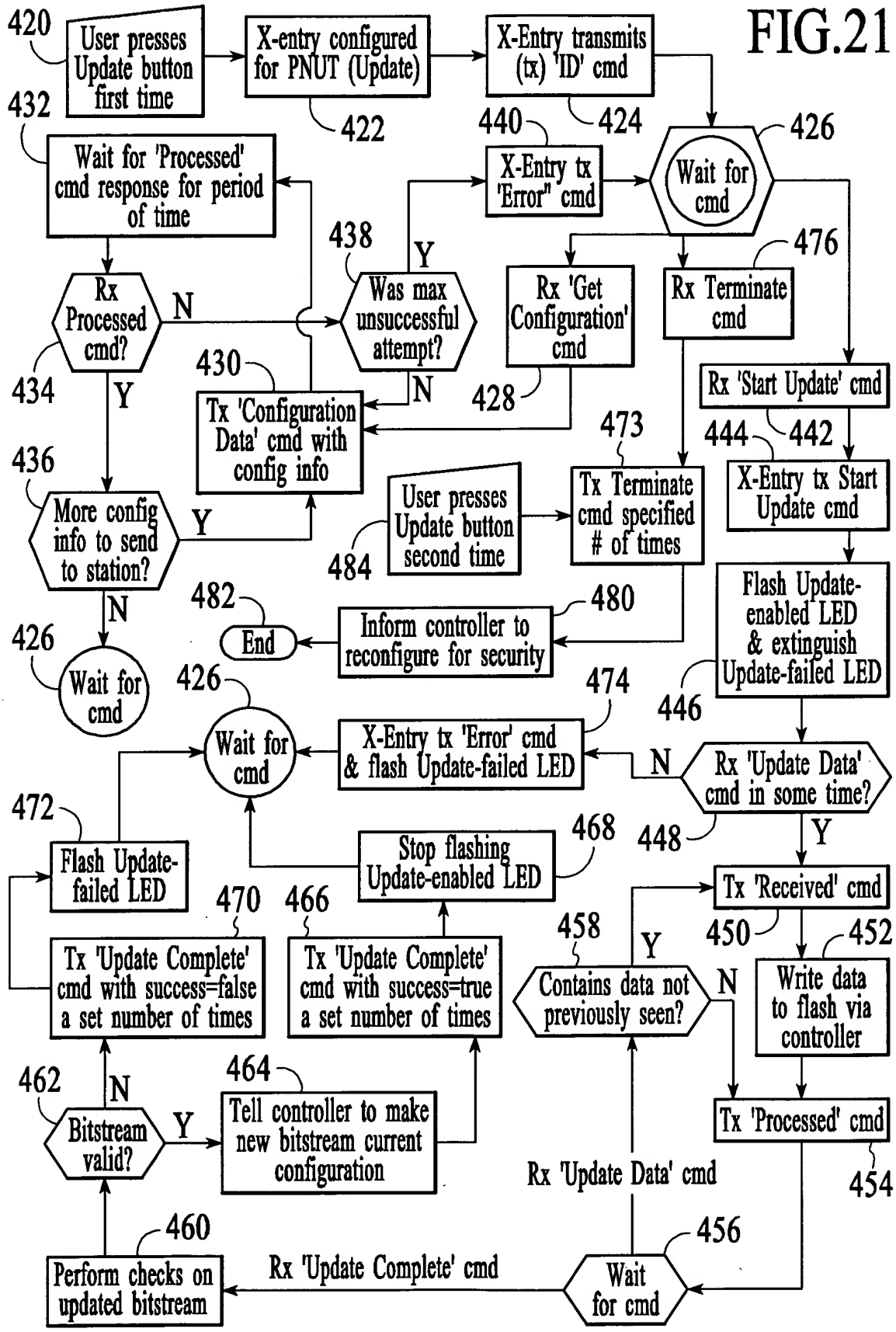

420
User presses Update button first time
X-entry configured for PNUT (Update)
422
X-Entry transmits (tx) 'ID' cmd
424
426
Wait for cmd
440
X-Entry tx 'Error" cmd
432
Wait for 'Processed' cmd response for period of time
438
Y
Was max unsuccessful attempt?
N
Rx Processed cmd?
N
434
Y
430
Tx 'Configuration Data' cmd with config info
428
Rx 'Get Configuration' cmd
476
Rx Terminate cmd
Rx 'Start Update' cmd
444
442
X-Entry tx Start Update cmd
473
Tx Terminate cmd specified # of times
436
More config info to send to station?
Y
User presses Update button second time
484
N
482
End
480
Inform controller to reconfigure for security
Flash Update-enabled LED & extinguish Update-failed LED
446
426
Wait for cmd
474
X-Entry tx 'Error' cmd & flash Update-failed LED
N
Rx 'Update Data' cmd in some time?
448
Y
472
Flash Update-failed LED
468
Stop flashing Update-enabled LED
Tx 'Received' cmd
450
452
458
Y
470
466
Tx 'Update Complete' cmd with success=false a set number of times
Tx 'Update Complete' cmd with success=true a set number of times
Contains data not previously seen?
N
Write data to flash via controller
462
N
464
Bitstream valid?
Y
Tell controller to make new bitstream current configuration
Tx 'Processed' cmd
454
Rx 'Update Data' cmd
460
456
Perform checks on updated bitstream
Rx 'Update Complete' cmd
Wait for cmd

FIG.21

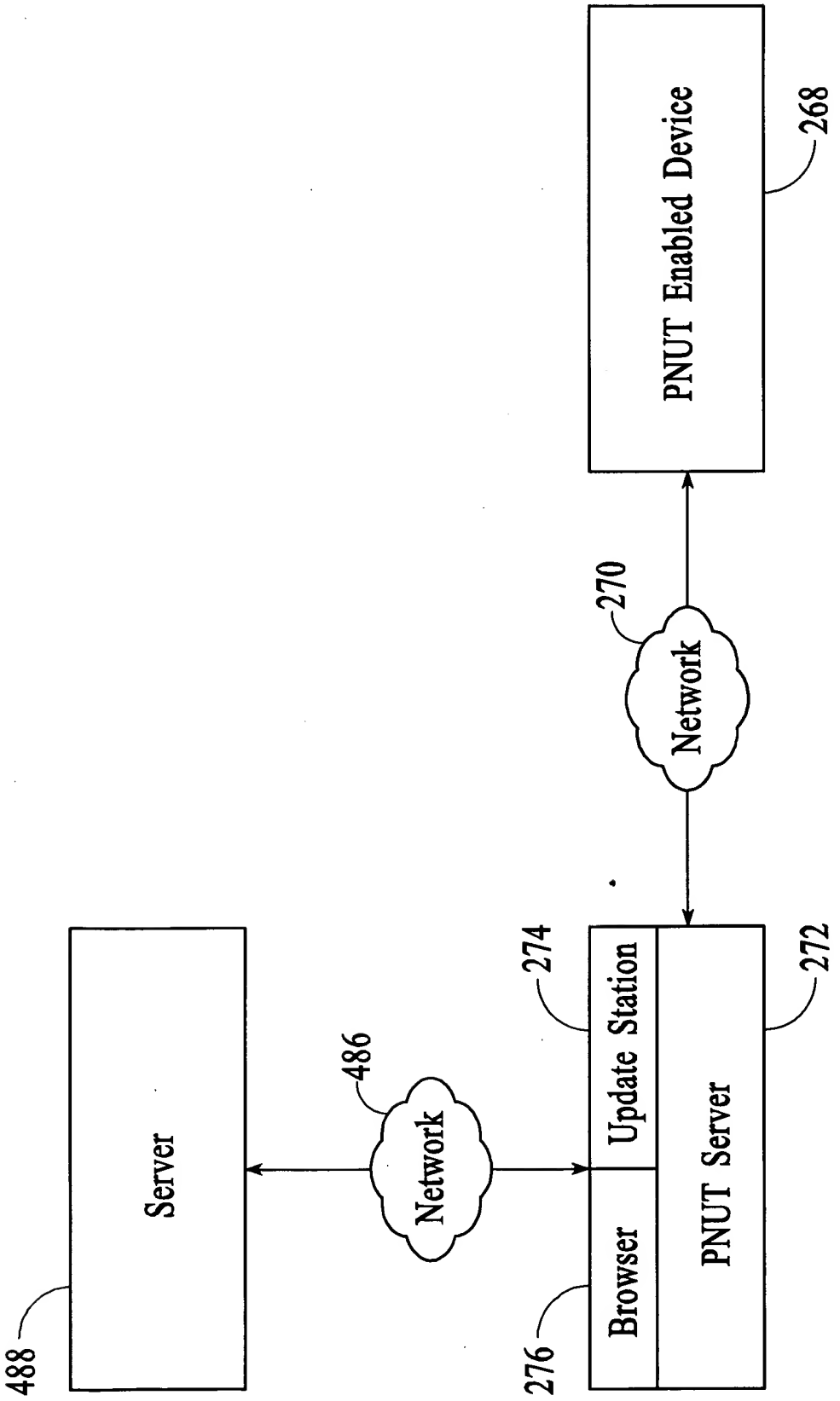

PNUT Enabled Device
268
270
Network
Server
488
486
Network
274
Update Station
Browser
276
PNUT Server
272

FIG.22

```
<?xml version = "1.0" encoding = "UTF-8"?>
<formats>
  <msg id = "128" name = "UPDATE_START_CMD">
    <desc> Start PNUT update</desc>
    <byte name = "type" transient = "true" />
    <bytes name = "checksum" size = "2" />
  </msg>
  <msg id = "129" name = "UPDATE_MSG_CMD">
    <desc> PNUT data update packet </desc>
    <bytes name = "packet number" size = "2" />
    <bytes name = "length" size = "2" transient = "true" />
    <bytes name = "data" min_size = "1" max_size = "500"
     transient = "true" max_print = "0" />
  </msg>
  <msg id = "130" name = "UPDATE_LAST_MSG_CMD">
    <desc> Last PNUT update packet </desc>
    <bytes name = "packet number" size = "2" transient = "true" />
    <pad size = "8" />
  </msg>
  <msg id = "132" name = "UPDATE_CNX_CMD">
    <desc> Cancel PNUT update </desc>
    <pad size = "24" />
  </msg>
  <msg id = "136" name = "UPDATE_COMP_CMD">
    <desc> PNUT update complete </desc>
    <bytes name = "status" size = "1" transient = "true">
      <status success = "0">
        <desc val = "0">Successful</desc>
        <desc val = "1">Bad packet checksum</desc>
        <desc val = "2">Flash write failure</desc>
        <desc val = "3">Update cancelled</desc>
      </status>
    </bytes>
    <pad size = "16" />
  </msg>
</formats>
```


FIG.23

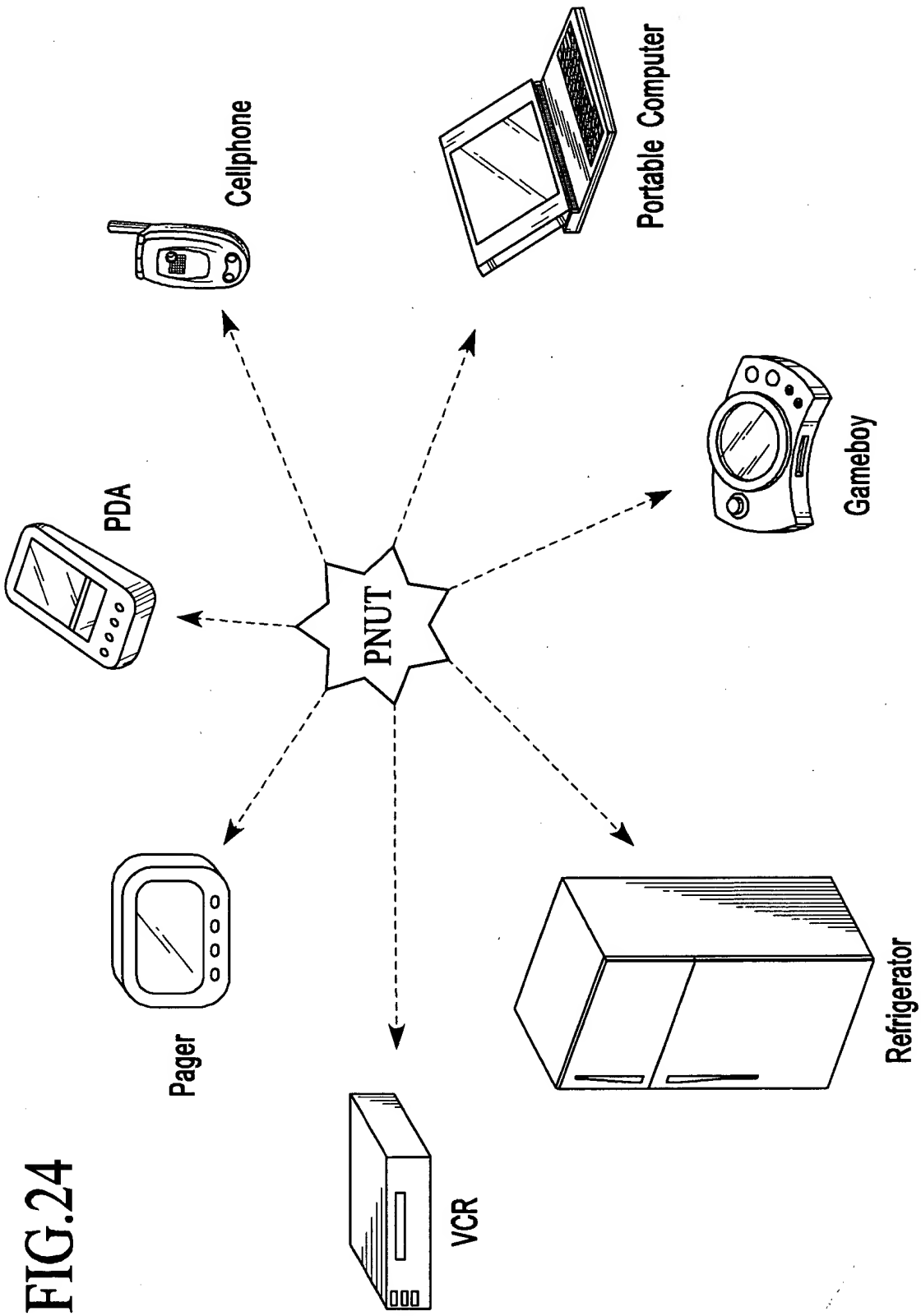

Cellphone
Portable Computer
PDA
PNUT
Gameboy
Pager
Refrigerator
VCR

FIG.24